2021 PAPER REVIEW

8월 1주차 미팅

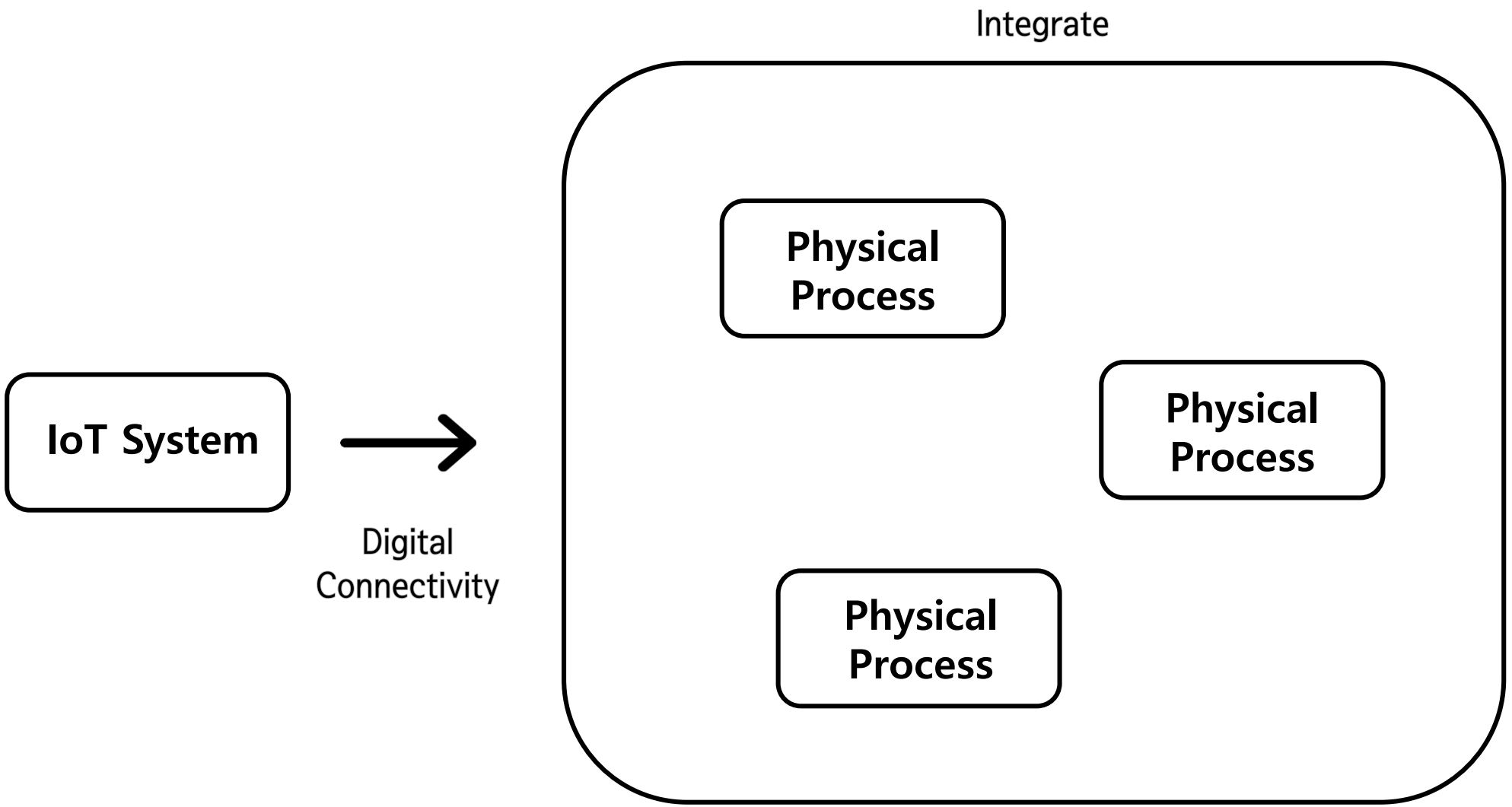
ICT 융합학부
202005414 지훈

선정 논문

IoTGUARD : Dynamic Enforcement of Security and Safety Policy in Commodity IoT

Published on NDSS SYMPOSIUM 2022

IoT Platform



IoT Platform

These IoT Systems structure the architecture **from bottom to top**

HUB as Main Gateway

Cloud

Interface

IoT Platform

IoT Device

Actuator

IoT Platform

Physical State →

Protocol

Send **Event** →

Another Device

HUB

CLOUD

IoT Programming Platform

SmartThings

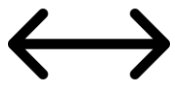
HomeKit

thingworx

openHAB
empowering the smart home

Trigger - Action Platform

Physical Process

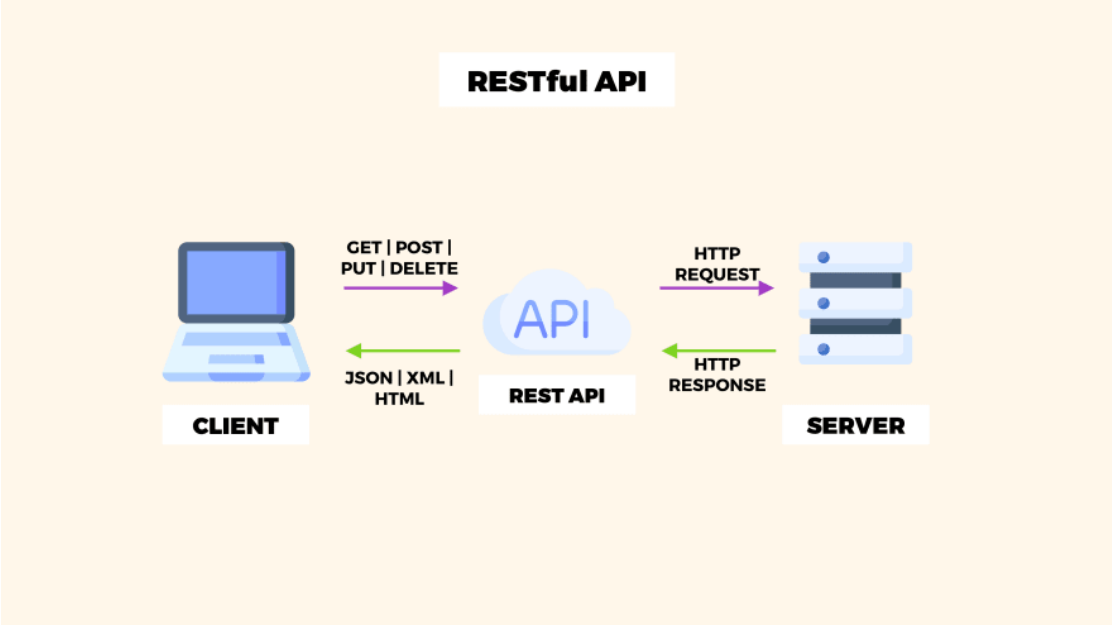


Digital Process

Trigger - Action Platform

If user allow the service, services communicate with each other using **REST API**

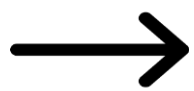
REST API : A very simple **interface** for **transferring data on the web over HTTP** without a **separate transport layer**



Trigger - Action Platform

DO rules

IF rules



Custom
Automation

Trigger - Action Platform

DO rules → Act like a **Button Trigger** to take sets of actions

e.g) Turn on the smart switch “**when the button is pressed**”

IF rules → Combine two services That use **Trigger and Action**

e.g) Call security guard when motion sensors detect motion “**after midnight**”

Terms

Attribute → Set of **“STATE”**

e.g) OPENING, OPENED, CLOSING, CLOSED

Action → Simple act

e.g) OPEN, CLOSE

Event → Triggered when **STATE changes**

Terms of Interaction

1) When an event handler of an app changes a device attribute, which triggers another event **that is subscribed to by another app**

e.g) One app **turns on the lights** when there's smoke, and the another one **opens the door** when it's lit

2) When multiple apps change the **same device attribute**

e.g) While the smoke alarm app **opens the water valve** to activate the sprinkler, the leak detection app sometimes **locks the water valve** when there is a leak

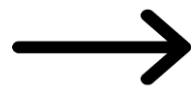
3) When apps that **subscribe to the same event** change a device attributes **in conflicting ways**

e.g) When the motion is enabled, when the **one app turns off the switch**, **one app turns on the switch**

IoT Platform

Interaction Between Devices through **abstract event**

Direct Interaction Between Devices



Safety and Security Violation

Undesirable State

FireWall

Intrusion Detection

Access Control Policy

SoftWare Patch

→ Strengthen **Perimeter Defense**

Does not guarantee the **safe operation of physical process**

Both **Dynamic and Static Approaches are problematic**

Dynamic Policy-Based

IoTGUARD

1) Implement a **code instrument** that adds logic to the app's source code to **collect information from the app in runtime**

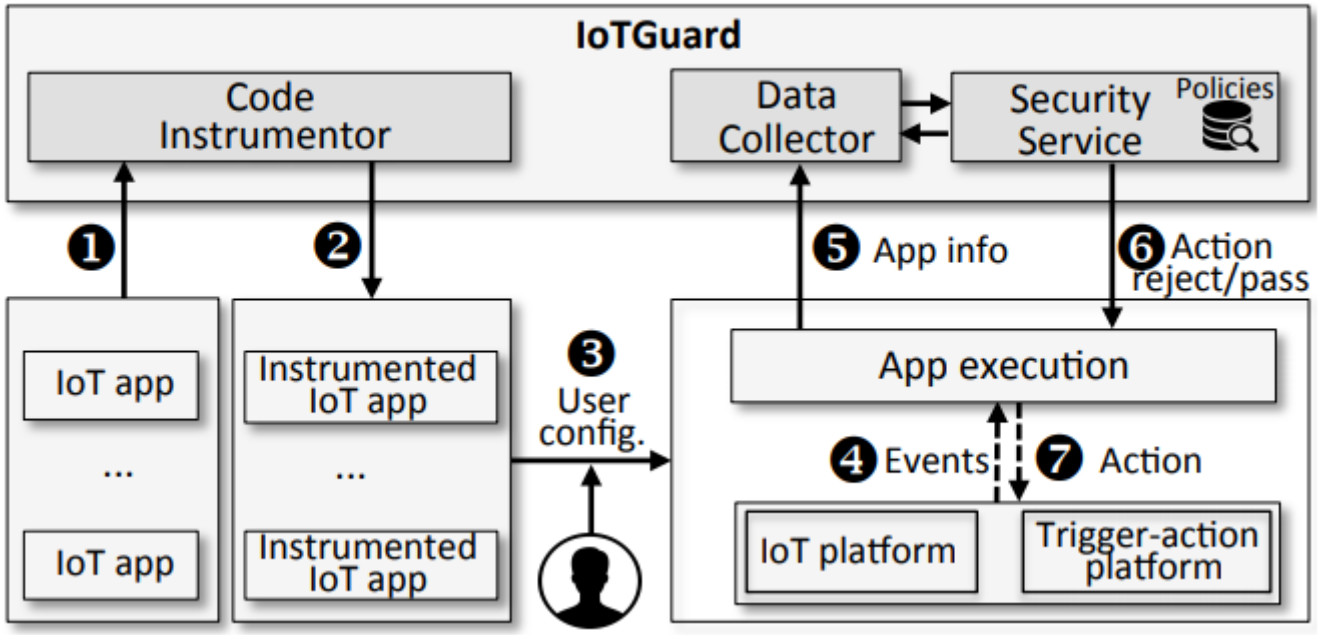
2) Store app information **in a dynamic model** that represents the **runtime execution behavior of apps**

3) Check **IoT safety and security policies,** execute relevant policies on dynamic models of **individual apps or sets of apps**

4) Reject or Pass the action by checking if **the policy is violated or if the state is not desired**

Dynamic Policy-Based

IoTGUARD



Dynamic Policy-Based

IoTGUARD

High-Level state block effect and **low runtime overhead requirements**

1) Valid for all **20 Defective apps** created by themselves

2) Runtime overhead of **17.3% in individual apps** and **19.8% in five interaction apps**

Thank you